# The Evolving Cybersecurity Landscape: Industry Perspectives on Securing the Nation's Infrastructure

**Incident Command System for Industrial Control Systems (ICS4ICS)**

Committee on Transportation and Infrastructure

Thursday, November 4, 2021, at 10:00 a.m. (EDT)

**Megan Samford**

Advisory Board Chairperson, ISA Global Cybersecurity Alliance (ISAGCA)

Chairperson, Incident Command System for Industrial Control Systems (ICS4ICS)

VP, Chief Product Security Officer – Energy Management, Schneider Electric

Co-Chair, Department of Homeland Security Control Systems Working Group

## Introduction

Chairman DeFazio, Ranking Member Graves, and Members of the Committee on Transportation and Infrastructure, on behalf of the International Society of Automation Global Cybersecurity Alliance – the ISAGCA-- and its over 50 public-and private sector automation and cybersecurity member organizations that cross all 16 critical infrastructure sectors and comprise over $1.5 trillion in aggregate revenue, thank you for the opportunity to testify on "Incident Command System for Industrial Control Systems" (ICS4ICS).

## Abstract

The private sector lacks a consistent, repeatable, and scalable framework to respond to day to day cyber incidents as well as cyber incidents where the impact spans partners, suppliers, customers, and coordination with local, state, and federal government. In the event of a large-scale cyber incident, this deficiency can lead to poorly executed responses that have impacts on lives and property.

The goal of "Incident Command System for Industrial Control Systems," which we refer to as ICS4ICS, is to identify how the private sector can adopt portions of the National Incident Management System (NIMS) Incident Command System (ICS) to ensure coordinated, uniform and more effective cyber-incident response. [1] Implementing ICS4ICS at scale will help the United States more effectively coordinate cyber incident response and recovery efforts within the private sector, especially for critical infrastructures.

[1] *IS-100.C: Introduction to the incident command system, ICS 100*. Federal Emergency Management Agency | Emergency Management Institute. (n.d.). Retrieved October 28, 2021, from https://training.fema.gov/is/courseoverview.aspx?code=is-100.c.

Together with the United States Department of Homeland Security Cyber and Infrastructure Security Agency (CISA), the ISAGCA and its member organizations such as Schneider Electric, Rockwell Automation, Johnson Controls International, Honeywell, Ford Motor Company, Pfizer, Exelon, Mandiant, Dragos, ClarOTy, Nozomi, and Idaho National Labs, have established a public-private partnership to deliver the ICS4ICS cyber-incident response framework. [2]

The success of the program thus far indicates that it provides value for both the private sector as well as government. This is evidenced by the number of daily, active volunteers, contributed by both the private sector and government. In a little over a year from its creation, the program has proven that it is possible to apply the NIMS Incident Command System framework to cyber-incident responses in the private sector, credential and type cyber-incident response roles into a common response structure (similar to fire and emergency services), as well as create draft common response templates to speed up responses and reduce error. This is all being done on volunteer time because the membership of this understands how badly the lack of scalability in cyber-incident response is hurting industries both in the United States, as well as globally.

While we are pleased with the rate at which the program is growing through the ISAGCA, we recognize that to make it adoptable at scale, we need the bi-partisan support of this Congress in developing a path for the program to be transitioned to operations within the United States government.

[2] Greig, J. (2021, July 13). *Cybersecurity organizations announce New First Responder Credentialing program*. ZDNet. Retrieved November 1, 2021, from https://www.zdnet.com/article/cybersecurity-organizations-announce-new-first-responder-credentialing-program/.

My name is Megan Samford.

As the Advisory Board Chair of the ISA Global Cybersecurity Alliance, I am representing the member organizations that are strongly committed to securing the industrial control systems that are the heart and lungs of not only American but global critical infrastructures. As a global organization, members of the ISAGCA are all aligned around the ISA/IEC 62443 standard for cybersecurity for industrial automation. I am also the Vice President of Product Cybersecurity and Chief Product Security Officer for Schneider Electric's Energy Management business. Schneider Electric was a founding member of the ISAGCA and is committed to ensuring the efficiency, resiliency, sustainability, and cybersecurity of electric grids globally. Lastly, I am Co-Chair of the US Department of Homeland Security's Control Systems Working Group within the Cybersecurity and Infrastructure Security Agency (CISA).

My background in emergency and incident management dates back to 2007, when I graduated from Virginia Commonwealth University as one of the first 50 individuals in the United States with a Bachelor of Art's degree in Homeland Security and Emergency Preparedness. From there, I worked under Governors Tim Kaine and Bob McDonnell, lastly serving as Virginia's Critical Infrastructure Protection (CIP) Coordinator. During this time, I had great exposure to traditional physical security and emergency management principles, to include the NIMS Incident Command System, which I will refer to as "ICS" moving forward. I saw firsthand by working in the Virginia Emergency Operations Center (VEOC) that ICS was a great way to efficiently coordinate responses and I began to adapt much of the work I was doing in Critical Infrastructure Protection planning to model ICS principles. My first attempt at more closely integrating private sector response capabilities was in an article I published in 2014 titled, "Framework for the Integration of Emergency Support Function, Infrastructure Protection and Supply Chain Management Efforts" which aimed to describe how the private sector could "hook into" local, state, and federal disaster response efforts through integration with state level Emergency Operation Center Emergency Support Functions (ESFs). [3] As such, the effectiveness and efficiency of coordinated responses between the private and public sectors has been a focus area of my work for nearly the past decade.

Because of my background in critical infrastructure protection and focus on government and private sector collaboration, I was recruited into the private sector to help companies build and implement product cybersecurity programs, of which response has always been a strong element. I've had roles at both the tactical and strategic levels of program design and implementation, I've worked for the top manufacturers of Industrial Control Systems products and systems, and now I'm working on my third product security program, at Schneider Electric's Energy Management Business.

Most recently, and what I am happy to testify on today, I became one of four cybersecurity first responders to be formally credentialed under the United States National Incident Management System Incident Command System as a Type I Cyber Incident Commander. This role plays a critical function in leading and directing cyber-incident responses as well as ensuring proper span and control, and resourcing. I am one of only four the United States has, and one of only

[3] Samford, M. (2014). Framework for the Integration of Emergency Support Function, Infrastructure Protection and Supply Chain Management Efforts. Homeland Security Today.

two within the private sector: The other two are within the United States Army Reserves Innovation Command the United States Department of Homeland Security, respectively.

- *Mark Bristow*, Branch Chief, United States Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA)
- *Colonel Brian Wisniewski*, US Army Reserves Innovation Command G2/G6
- *Neal Gay*, Senior Manager, Managed Defense, Mandiant
- *Megan Samford*, Vice President, Product Cybersecurity, Schneider Electric

Today, I hope to tell you what the ICS4ICS program is, why the United States government and private sector needs it, and why this effort needs a home in the United States government to scale.

## What is ICS4ICS?

ICS is a standardized, repeatable, and scalable approach to managing both day-to-day and complex incidents. It was created here in the United States during the 1970s as a result of the California Wildfire responses, where multiple fire departments and state and federal agencies had come together to respond in a unified and coordinated way.[4] ICS has been tested in more than 40 years of emergency and nonemergency applications by all levels of government and in the private sector. At its foundation, ICS recognizes a need for different organizations to work together toward common goals.

[4] *ICS 100 – Incident Command System - USDA*. (n.d.). Retrieved October 28, 2021, from https://www.usda.gov/sites/default/files/documents/ICS100.pdf.

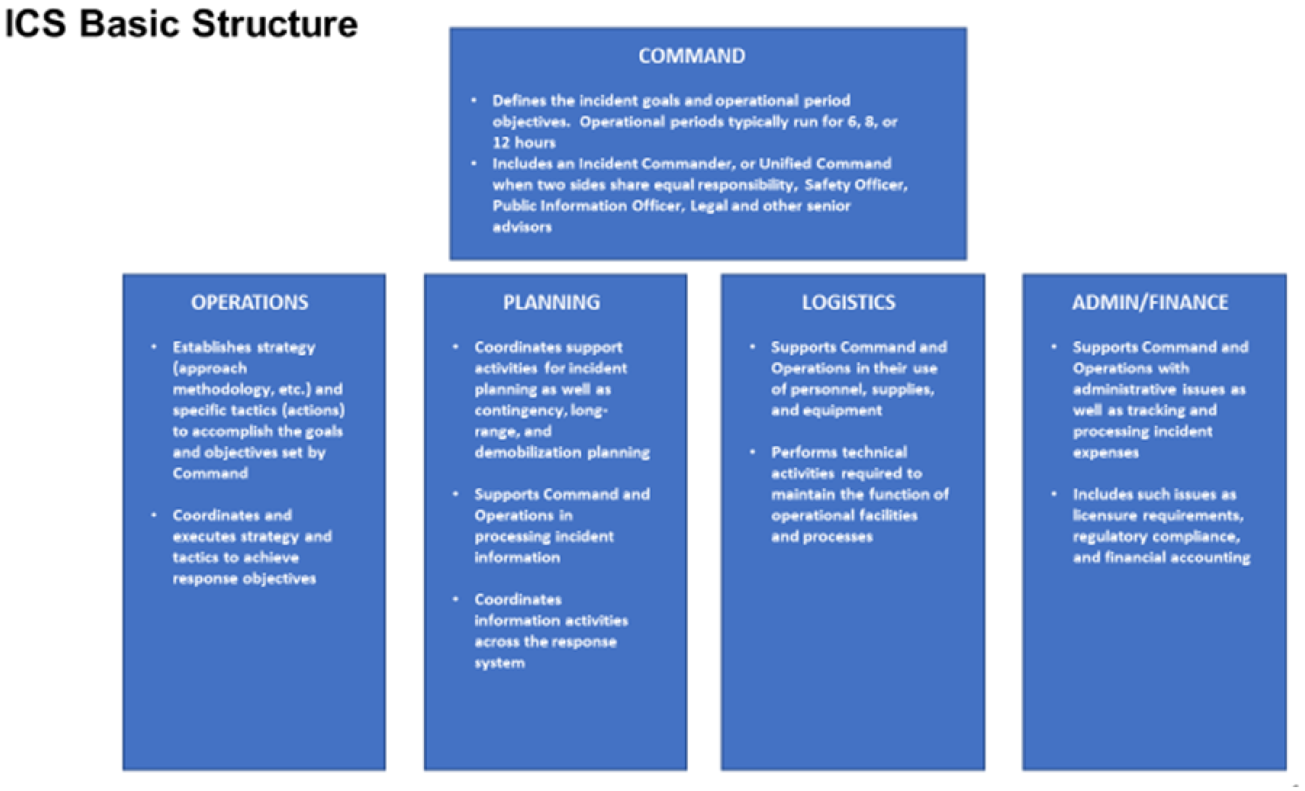
ICS addresses:

- Nonstandard terminology among responding entities
- Lack of capability to expand and contract as required
- Lack of an orderly, systemic planning processes
- Nonstandard & nonintegrated communications
- Lack of personnel accountability, including unclear chains of command and supervision
- No common, flexible, predesigned management structure that enables commanders to delegate responsibilities and manage workloads efficiently

In preparing for this testimony, I found the below expert from the United States Department of Agriculture Incident Command System 101 Course material to be very helpful in plainly explaining what Incident Command System is.

> "The Incident Command System or ICS is a standardized, on-scene, all-risk incident management concept. ICS allows its users to adopt an integrated organizational structure to match the complexities and demands of single or multiple incidents without being hindered by jurisdictional boundaries. ICS has considerable internal flexibility. It can grow or shrink to meet different needs. This flexibility makes it a very cost effective and efficient management approach for both large and small incidents. Designers of the system recognized early that ICS must be interdisciplinary and organizationally flexible to meet the following management challenges:
>
> - Meet the needs of incidents of any kind or size
> - Be useable or repeatable for routine or planned events such as conferences, as well as large and complex emergency incidents

- Allow personnel from a variety of agencies to meld rapidly into a common management structure
- Provide logistical and administrative support to ensure that operational staff, such as Forensic investigators and malware reverse engineers, can meet tactical objectives
- Be cost effective by avoiding duplication of efforts” [4]



ICS Basic Structure

COMMAND

- Defines the incident goals and operational period objectives. Operational periods typically run for 6, 8, or 12 hours
- Includes an Incident Commander, or Unified Command when two sides share equal responsibility, Safety Officer, Public Information Officer, Legal and other senior advisors

OPERATIONS

- Establishes strategy (approach methodology, etc.) and specific tactics (actions) to accomplish the goals and objectives set by Command
- Coordinates and executes strategy and tactics to achieve response objectives

PLANNING

- Coordinates support activities for incident planning as well as contingency, long-range, and demobilization planning
- Supports Command and Operations in processing incident information
- Coordinates information activities across the response system

LOGISTICS

- Supports Command and Operations in their use of personnel, supplies, and equipment
- Performs technical activities required to maintain the function of operational facilities and processes

ADMIN/FINANCE

- Supports Command and Operations with administrative issues as well as tracking and processing incident expenses
- Includes such issues as licensure requirements, regulatory compliance, and financial accounting

The above chart explains the five basic management functions within ICS: Command, Operations, Planning, Logistics, and Admin/Finance.   As incidents expand, additional sub structures can be broken out to support scaling incidents. The functions apply in both small-and large-scale incidents.

A key principle within the application of the management functions is span of control.  No one leader can have more than seven people directly reporting to them to ensure span of control.

This helps to ensure accountability and reduce confusion during responses. [4] Of note, is that as incidents contract, the organization can scale down accordingly, until only a few responders remain to support the incident. [4]

Since its early adoption in the 1970s, to its full adoption across the public sector today through the Federal Emergency Management Agency (FEMA), the Incident Command System has saved thousands of lives, businesses, and property; has been endorsed by the United Nations; and now, the most developed countries in the world follow this system for emergency management.[5] Every local fire, EMS, state agency, and federal response entities in the US follow and know ICS by heart – it's simply how we respond.

Additionally, many private sector organizations now use ICS to run day-to-day operations, planned events, as well as responses because of its proven effectiveness in safety critical environments. This is particularly common within electric utility companies. ICS has been a gift to the world and the United States should be proud of this proven response framework.

## The Private Sector Cyber-Incident Response Problem – Scaling & Interoperability

Having worked in product security programs for nearly a decade, I speak from experience when I say that while individual companies may have a cyber response plan, or "playbook" as they are commonly referred, that is robust and effective, these plans often suffer during larger crisis because of a lack of coordination capacity that can scale outside of their organization, and their

[5] Millner, G. C., & Murta, T. L. (n.d.). *Incident management*. Incident Management - an overview | ScienceDirect Topics. Retrieved October 28, 2021, from https://www.sciencedirect.com/topics/nursing-and-health-professions/incident-management.

control. [6] Each plan is unique to the organization and defines who does what within the organization, notification procedures, technical team capabilities, interaction with legal and communications, and regulatory requirements – the playbooks are comprehensive, but written on a company-by-company basis and lack interoperability. Existing cybersecurity standards do not specifically address a larger response framework concept like ICS.

The breakdown with this planning approach occurs when the response is larger than one organization. The individual plans cannot scale effectively into a collaborative response when multiple companies, jurisdictions, and government entities need to be brought to bear for a large-scale attack scenario. The Solar Winds supply chain attack highlights the trend that cross-company, cross-sector, multiple party responses are on the rise. Currently, there is no repeatable and consistent framework to support cyber-incident response interoperability among the stakeholders.

## What are the larger impacts of not having a common framework?

The larger impacts for both the private sector and the government of not having a common framework are that disasters can become catastrophes when the responses cannot be contained. The consequences of not having a structure like ICS4ICS can lead to inefficient and costly responses, both for life and property due to a lack of a common response framework.

From my observations, for the private sector:

[6] Singh, A. *What are cyber incident response playbooks & why do you need them?* APMG International. Retrieved October 28, 2021, from https://apmg-international.com/article/what-are-cyber-incident-response-playbooks-why-do-you-need-them.

- There lies an inability for responses to scale outside of one or two organizations. No larger structure exists for the private sector to share resources through mutual aid agreements.
- There is no standard terminology, "common language", or common response templates. Common language and templates help to speed up responses and lessen confusion. Lack of communications interoperability was cited in the Implementing Recommendations of the 9/11 Commission Act of 2007. [7]
- There are no "typed" cyber-incident responder roles. Typing is a way of characterizing roles so that they are shared across a function. Example: A Type 1 Incident Management Team in Virginia has essentially the same training and experience as a Type 1 Incident Management Team in California. This creates baseline capability and understanding and is a foundational premise of Incident Command System.
- The private sector playbooks are based on traditional enterprise information technology and are focused on tactical actions needed to mitigate harm to the organization, gather evidence, and determine what internal and external escalations/notifications are needed.
- Time and resources are not well tracked or managed resulting in response fatigue, and hindered decision making over extended operational periods. Surge capacity is rarely available to provide relief, which also compounds response fatigue.

From my observations, what this in turn means for the government is:

[7] *Implementing recommendations of the 9/11 ... - congress.gov*. (n.d.). Retrieved October 28, 2021, from https://www.congress.gov/110/plaws/publ53/PLAW-110publ53.pdf.

- Out of the many defined natural and man-made disaster types, cyber is the only disaster type that currently does not follow Incident Command System.
- If 85% of critical infrastructures are owned and operated within the private sector, the US government lacks a way to effectively coordinate under a common structure with a large percentage of its cyber response resources.
- There is a lack of understanding of the degree of cyber expertise and capability the private sector could bring to bear.

If you take the example of the Colonial Pipeline ransomware attack, the asset owner and operator had detected ransomware on the enterprise network and made the decision to safely shut down pipeline operations to prevent the potential spread of the ransomware into that safety critical environment. For all intents and purposes, this was a responsible decision given the information available to decision makers at that time. What we see in this scenario is that the major impacts of the attack occurred not from the inherent ransomware attack, but from the cascading impacts of proactively shutting down the pipeline. Again, "disasters become catastrophes when responses cannot be contained".

While shutting down pipeline operations was the appropriate and safe decision, the cascading impacts of that decision meant the response became less centralized because other impacted organizations, such as the United States Department of Homeland Security, were brought in to support the response. While I was not personally involved in the response and remediation efforts, it can be inferred from the aftermath that a unified public and private coordination structure could have resulted in increased public confidence over the response. The lack of public confidence and trust contributed to reactionary demand for gas, resulting in shortages.

While the Colonial Pipeline example demonstrates how large responses can scale, even for mature and well-resourced organizations, in many cases, smaller organizations face even larger resource constraints. A system like ICS4ICS can help companies provide mutual aid to one another. This is not unlike how electric utility companies share lineman during power restoration efforts following hurricanes. You frequently see lineman from Dominion Energy based in Virginia support hurricane recovery efforts in Florida. As such, the electric utilities are also investigating the use of ICS4ICS: Sharing resources is a well understood concept for that industry.

## The idea of ICS4ICS

Given these critical gaps and my past experience as an emergency manager, I had the idea to apply the NIMS Incident Command System framework and train cyber-incident responders in the same way we train every other first responder in the United States. I put pen to paper and drafted a cyber-incident coordination framework that could be applied to cyber-incident responses based on Incident Command System.

After I introduced the ICS4ICS idea at one of the largest Industrial Control Systems Cybersecurity conference in the world, the ISAGCA agreed to pick up the effort and it has grown: We now have training programs on ICS4ICS, have updated response templates, and we are educating cybersecurity experts on the framework.

## Approach of ICS4ICS in Delivering Cyber Response Capability to the Private Sector

Through ICS4ICS we are encouraging member organizations to start adoption by overlaying this organizational structure over their current response playbooks. We are not suggesting that ICS4ICS become a replacement for existing response playbooks; instead, the Incident Command

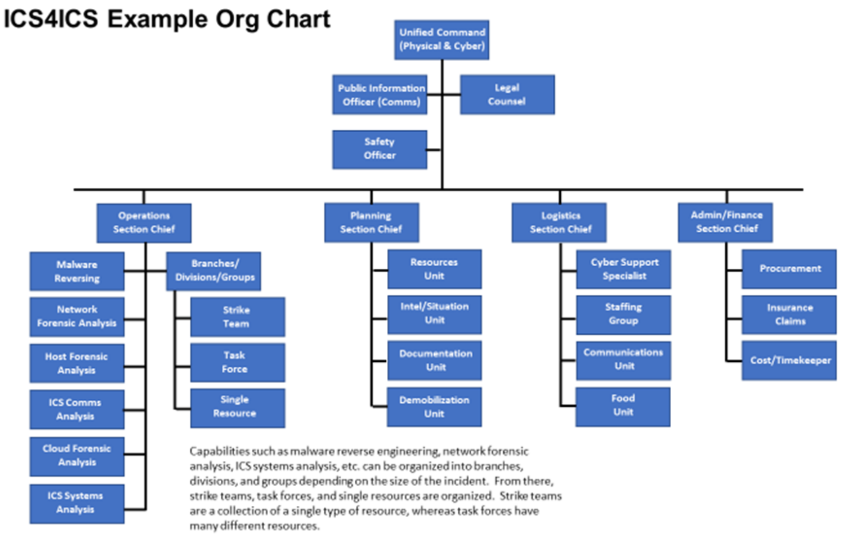
System should be applied as a higher-level way of structuring command and control as well as management of resources. The typing of resources is also significant as it enforces common terminology and expectations for each typed role.

Currently ICS4ICS has over 350 cyber volunteers registered to become credentialed - most within the United States but there has been increasing interest from cyber security experts in Europe, Canada, Latin America, Asia, Australia, and New Zealand. These international groups will likely stand up their own local implementation and credentialing processes. To become credentialed, a cyber-incident responder must:

- Submit an application to ICS4ICS
- Create an account through FEMA's One Responder system
- Complete 18 hours of online FEMA ICS training (the courses may be able to be shortened at a later date)
- Complete the Position Task Book application clearly demonstrating where the applicant has obtained experience working cyber-incidents (a third-party verification is required to be filled out by a former supervisor or person in an authority role for the described cyber-incident)

Once the application is completed, the applicant will receive notice of the opportunity to appear before the ICS4ICS adjudication committee (includes a representative from DHS CISA) to discuss their application and answer any questions the adjudication committee may have. Once approved, the credential is assigned and documented within the FEMA One Responder portal.

Below is an example template that can be used by the private sector when organizing a response in an Operational Technology (OT) environment:


ICS4ICS Example Org Chart

Capabilities such as malware reverse engineering, network forensic analysis, ICS systems analysis, etc. can be organized into branches, divisions, and groups depending on the size of the incident. From there, strike teams, task forces, and single resources are organized. Strike teams are a collection of a single type of resource, whereas task forces have many different resources.

The next phase of the program will include continued creation of response plan templates, hazard specific annexes to support events like ransomware, Incident Action Plan templates, and needed credentialing. DHS will also need to decide if private sector companies with trained cyber-incident responders should integrate into the current NIMS, state multi-agency coordination center (MACC) model, or if a centralized office should be created within DHS.

## Closing

Poorly managed cyber-incident responses can be devastating to our national security, health and safety, and economy. Even after twenty years, many of the same response challenges that faced emergency responders on 9/11 continue to be challenges for us now, except in cyber-incident response – lack of common response frameworks and interoperability. With so much at stake, we must effectively manage cyber-incidents, together, with both the private sector and government. The Incident Command System allows us to do so. [4]

This effort is ramping up quickly and deserves a home in the United States government. On behalf of the ICS4ICS effort, I respectfully request your bi-partisan support for this important program in requesting the government investigate ways to expand and enhance the spirit of language captured in Homeland Security Presidential Directive-5 to encourage adoption of Incident Command System within the private sector for cyber-incident response:

> "The Federal Government recognizes the role that the private and nongovernmental sectors play in preventing, preparing for, responding to, and recovering from terrorist attacks, major disasters, and other emergencies. The Secretary will coordinate with the private and nongovernmental sectors to ensure adequate planning, equipment, training, and exercise activities and to promote partnerships to address incident management capabilities." [8]

Additionally, we respectfully request that Congress make the necessary plans and investments for the private sector to become trained and credentialed in Incident Command System in the same way that fire and emergency services are trained today, and lastly, ICS4ICS be operationalized as an official government program, residing in the United States Department of Homeland Security, or another entity, if appropriate.

[8] *Homeland Security Presidential Directive 5*. (n.d.). Retrieved October 28, 2021, from https://www.dhs.gov/sites/default/files/publications/Homeland%20Security%20Presidential%20Directive%205.pdf.